CLAIMS

Having thus described our invention, what we claim as new and desire to secure by Letters Patent is as follows:

1. A computer-assisted method of generating at least one test procedure for a target system having at least one device capable of being identified, each of the at least one device having hardware and/or software, said method comprising the steps of:

a) collecting information descriptive of at least a hardware and/or software specification for the at least one device;

b) selecting at least one predefined standard, regulation and/or requirement with which the target system is to comply;

c) associating hardware and/or software information pertaining to the at least one device, collected in said step a), with at least one pre-defined platform category;

d) for each of said at least one platform category, determining which of one or more test procedures will be used to test hardware and/or software associated with said at least one platform category based on a mapping between the test procedures and the at least one predefined standard, regulation and/or requirement; and

e) generating one or more test procedures as determined in said step d) for each platform category.

2. The method according to claim 1 further comprising the step of associating at least one application software program with at least one platform category, the association indicating that the application program is typically installed on devices belonging to the platform category.

3. The method according to claim 1 wherein said step a) information is collected, for the target system comprising a plurality of devices within a network, by at least one of electronic discovery via a network and manual entry.

4. The method according to claim 3 wherein electronic discovery comprises an enterprise management system.

5. The method according to claim 3 wherein the information collected in said step a) pertains to at least one of: an internet protocol address, a hostname, a media access control address, an operating system name, and an operating system version.

6. The method according to claim 1 further comprising the step of editing said step a) information descriptive of at least the hardware specification and the operating system of each device.

7. The method according to claim 1 wherein the platform categories comprise at least one of desktop computer, laptop computer, mainframe computer, hub, handheld device, and other.

8. The method according to claim 1 further comprising the step of printing at least one test procedure generated in said step e).

9. The method according to claim 1 wherein said step e) generates one test procedure for a platform category when there are no devices associated therewith, and generates one test procedure for each device associated with a platform category having an indication that such device is to be tested.

10. The method according to claim 1 further comprising the steps of:

f) performing the steps associated with the test procedures generated in said step e) to determine whether the target system passes or fails the at least one the test procedure;

g) generating a score for each of a plurality of threat elements, each score indicating a likelihood of that threat element affecting and/or impacting the target system; and

h) (1) obtaining a threat correlation indication associated with said at least one test procedure, wherein said threat correlation indication indicates a relative potential of one or more given threats to exploit a vulnerability caused by a failure of the at least one test procedure, and

(2) determining a risk assessment by comparing each score generated in said step g) with a corresponding threat correlation indication of said step h) (1).

11. The method according to claim 10 wherein said scores for said step g) comprise at least one of:

i) negligible, wherein negligible indicates that the threat element is not applicable or has negligible likelihood of occurrence;

ii) low, wherein low indicates that the threat element has a relatively low likelihood of occurrence;

iii) medium, wherein medium indicates that the threat element has a medium likelihood of occurrence; and

iv) high, wherein high indicates that the threat element has a relatively high likelihood of occurrence.

12. The method according to claim 10 wherein said step g) threat elements comprise at least one of natural disaster elements, system failure elements, environmental failure elements, unintentional human elements, and intentional human elements.

13. The method according to claim 12 wherein the natural disaster threat elements comprise at least one of fire, flood, earthquake, volcano, tornado and lighting elements.

14. The method according to claim 12 wherein the system failure threat elements comprise at least one of a hardware failure, a power failure, and a communication link failure.

15. The method according to claim 12 wherein the environmental failure threat elements comprise at least one of temperature, power, humidity, sand, dust, shock, and vibration.

16. The method according to claim 12 wherein the human unintentional threat element comprises at least one of a software design error, a system design error, and an operator error.

17. The method according to claim 12 wherein the human intentional threat elements comprise at least one of an authorized system administrator, an authorized maintenance personnel, an authorized user, a terrorist, a hacker, a saboteur, a thief, and a vandal.

18. The method according to claim 10 wherein said step h) (1) threat correlation indication comprises at least one of the following scores:

i) negligible, wherein negligible indicates that the threat is not applicable to the vulnerability;

ii) low, wherein low indicates that the threat has a low potential to exploit the vulnerability;

iii) medium, wherein medium indicates that the threat has a potential to exploit the vulnerability; and

iv) high, wherein high indicates that the threat has a relatively high potential to exploit the vulnerability.

19. The method according to claim 18 wherein the risk assessment in said step h) (2) is determined in accordance with the following steps:

a) for each element in the project threat profile and corresponding element in the threat correlation pattern:

1) if a threat element as determined in said step g) is negligible and a corresponding element in the threat correlation indication as determined in said step h) is anything, then the overall risk of the element is negligible;

2) if a threat element score as determined in said step g) is low and the corresponding element in the threat correlation indication as determined in said step h) is negligible, then the overall risk of the element is low;

3) if a threat element score as determined in said step g) is low and the corresponding element in the threat correlation indication as determined in said step h) is low, then the overall risk of the element is low;

4) if a threat element score as determined in said step g) is low and the corresponding element in the threat correlation indication as determined in said step h) is medium, then the overall risk of the element is low;

5) if a threat element score as determined in said step g) is low and the corresponding element in the threat correlation indication as determined in said step h) is high, then the overall risk of the element is medium;

6) if a threat element score as determined in said step g) is medium and the corresponding element in the threat correlation indication as

determined in said step h) is negligible, then the overall risk of the element is negligible;

7) if a threat element score as determined in said step g) is medium and the corresponding element in the threat correlation indication as determined in said step h) is low, then the overall risk of the element is low;

8) if a threat element score as determined in said step g) is medium and the corresponding element in the threat correlation indication as determined in said step h) is medium, then the overall risk of the element is medium;

9) if a threat element score as determined in said step g) is medium and the corresponding element in the threat correlation indication as determined in said step h) is high, then the overall risk of the element is medium;

10) if a threat element score as determined in said step g) is high and the corresponding element in the threat correlation indication as determined in said step h) is negligible, then the overall risk of the element is negligible;

11) if a threat element score as determined in said step g) is high and the corresponding element in the threat correlation indication as determined in said step h) is low, then the overall risk of the element is medium;

12) if a threat element score as determined in said step g) is high and the corresponding element in the threat correlation indication as determined in said step h) is medium, then the overall risk of the element is high; and

13) if a threat element score as determined in said step g) is high and the corresponding element in the threat correlation indication as determined in said step h) is high, then the overall risk of the element is high; and

b) selecting the risk profile for the failed test procedure as being the highest overall risk element.

20. The method according to claim 19 further comprising the step of determining an overall system risk.

21. The method according to claim 20 wherein the overall target system risk is the highest overall risk element of each of one or more failed test procedures.

22. The method according to claim 20 further comprising the step of printing a documentation package that will enable a determination to be made whether the target system complies with the at least one predefined standard, regulation and/or requirement selected in said step b).

23. The method according to claim 22 wherein the documentation package includes a risk assessment for at least one failed test procedure.

24. The method according to claim 22 wherein the documentation package includes an overall target system risk.

25. In a general purpose computing system, a computer-assisted method of generating at least one test procedure for a target system having at least one device capable of being identified, each of the at least one device having hardware and/or software, said method comprising the steps of:

a) collecting information descriptive of at least a hardware and/or software specification for the at least one device;

b) selecting at least one predefined standard, regulation and/or requirement with which the target system is to comply;

c) associating hardware and/or software information pertaining to the at least one device, collected in said step a), with at least one pre-defined platform category;

d) for each of said at least one platform category, determining which of one or more test procedures will be used to test hardware and/or software associated with said at least one platform category based on a mapping between the test procedures and the at least one predefined standard, regulation and/or requirement; and

e) generating one or more test procedures as determined in said step d) for each platform category.

26. The system according to claim 25 further comprising the step of associating at least one application software program with at least one platform category, the association indicating that the application program is typically installed on devices belonging to the platform category.

27. The system according to claim 25 wherein said step a) information is collected, for the target system comprising a plurality of devices within a network, by at least one of electronic discovery via a network and manual entry.

28. The system according to claim 27 wherein electronic discovery comprises an enterprise management system.

29. The system according to claim 27 wherein the information collected in said step a) pertains to at least one of: an internet protocol address, a hostname, a media access control address, an operating system name, and an operating system version.

30. The system according to claim 25 further comprising the step of editing said step a) information descriptive of at least the hardware specification and the operating system of each device.

31. The system according to claim 25 wherein the platform categories comprise at least one of desktop computer, laptop computer, mainframe computer, hub, handheld device, and other.

32. The system according to claim 25 further comprising the step of printing at least one test procedure generated in said step e).

33. The system according to claim 25 wherein said step e) generates one test procedure for a platform category when there are no devices associated therewith, and generates one test procedure for each device associated with a platform category having an indication that such device is to be tested.

34. The system according to claim 25 further performing the steps of:

f) performing the steps associated with the test procedures generated in said step e) to determine whether the target system passes or fails the at least one the test procedure;

g) generating a score for each of a plurality of threat elements, each score indicating a likelihood of that threat element affecting and/or impacting the target system; and

h) (1) obtaining a threat correlation indication associated with said at least one test procedure, wherein said threat correlation indication indicates a relative potential of one or more given threats to exploit a vulnerability caused by a failure of the at least one test procedure, and

(2) determining a risk assessment by comparing each score generated in said step g) with a corresponding threat correlation indication of said step h) (1).

35. The system according to claim 34 wherein said scores for said step g) comprise at least one of:

i) negligible, wherein negligible indicates that the threat element is not applicable or has negligible likelihood of occurrence;

ii) low, wherein low indicates that the threat element has a relatively low likelihood of occurrence;

iii) medium, wherein medium indicates that the threat element has a medium likelihood of occurrence; and

iv) high, wherein high indicates that the threat element has a relatively high likelihood of occurrence.

36. The system according to claim 34 wherein said step g) threat elements comprise at least one of natural disaster elements, system failure elements, environmental failure elements, unintentional human elements, and intentional human elements.

37. The system according to claim 36 wherein the natural disaster threat elements comprise at least one of fire, flood, earthquake, volcano, tornado and lighting elements.

38. The system according to claim 36 wherein the system failure threat elements comprise at least one of a hardware failure, a power failure, and a communication link failure.

39. The system according to claim 36 wherein the environmental failure threat elements comprise at least one of temperature, power, humidity, sand, dust, shock, and vibration.

40. The system according to claim 36 wherein the human unintentional threat element comprises at least one of a software design error, a system design error, and an operator error.

41. The system according to claim 36 wherein the human intentional threat elements comprise at least one of an authorized system administrator, an authorized maintenance personnel, an authorized user, a terrorist, a hacker, a saboteur, a thief, and a vandal.

42. The system according to claim 34 wherein said step h) (1) threat correlation indication comprises at least one of the following scores:

i) negligible, wherein negligible indicates that the threat is not applicable to the vulnerability;

ii) low, wherein low indicates that the threat has a low potential to exploit the vulnerability;

iii) medium, wherein medium indicates that the threat has a potential to exploit the vulnerability; and

iv) high, wherein high indicates that the threat has a relatively high potential to exploit the vulnerability.

43. The system according to claim 42 wherein the risk assessment in said step h) (2) is determined in accordance with the following steps:

a) for each element in the project threat profile and corresponding element in the threat correlation pattern:

1) if a threat element as determined in said step g) is negligible and a corresponding element in the threat correlation indication as determined in said step h) (2) is anything, then the overall risk of the element is negligible;

2) if a threat element as determined in said step g) is low and the corresponding element in the threat correlation indication as determined in said step h) (2) is negligible, then the overall risk of the element is low;

3) if a threat element as determined in said step g) is low and the corresponding element in the threat correlation indication as determined in said step h) (2) is low, then the overall risk of the element is low;

4) if a threat element as determined in said step g) is low and the corresponding element in the threat correlation indication as

determined in said step h) (2) is medium, then the overall risk of the element is low;

5) if a threat element as determined in said step g) is low and the corresponding element in the threat correlation indication as determined in said step h) (2) is high, then the overall risk of the element is medium;

6) if a threat element as determined in said step g) is medium and the corresponding element in the threat correlation indication as determined in said step h) (2) is negligible, then the overall risk of the element is negligible;

7) if a threat element as determined in said step g) is medium and the corresponding element in the threat correlation indication as determined in said step h) (2) is low, then the overall risk of the element is low;

8) if a threat element as determined in said step g) is medium and the corresponding element in the threat correlation indication as determined in said step h) (2) is medium, then the overall risk of the element is medium;

9) if a threat element as determined in said step g) is medium and the corresponding element in the threat correlation indication as determined in said step h) (2) is high, then the overall risk of the element is medium;

10) if a threat element as determined in said step g) is high and the corresponding element in the threat correlation indication as determined in said step h) (2) is negligible, then the overall risk of the element is negligible;

11) if a threat element as determined in said step g) is high and the corresponding element in the threat correlation indication as determined in said step h) (2) is low, then the overall risk of the element is medium;

12) if a threat element as determined in said step g) is high and the corresponding element in the threat correlation indication as determined in said step h) (2) is medium, then the overall risk of the element is high; and

13) if a threat element as determined in said step g) is high and the corresponding element in the threat correlation indication as determined in said step h) (2) is high, then the overall risk of the element is high; and

b) selecting the risk profile for the failed test procedure as being the highest overall risk element.

44. The system according to claim 43, further comprising the step of determining an overall system risk.

45. The system according to claim 44 wherein the overall target system risk is the highest overall risk element of each of one or more failed test procedures.

46. The system according to claim 44 further comprising the step of printing a documentation package that will enable a determination to be made whether the target system complies with the at least one predefined standard, regulation and/or requirement selected in said step b).

47. The system according to claim 46 wherein the documentation package includes a risk assessment for at least one failed test procedure.

48. The system according to claim 46 wherein the documentation package includes an overall system risk.

49. A computer program medium storing computer instructions therein for instructing a computer to perform a computer-implemented and user assisted process of generating at least one test procedure for a target system having at least one device capable of being identified, each of the at least one device having hardware and/or software, said program medium comprising the steps of:

a) collecting information descriptive of at least a hardware and/or software specification for the at least one device;

b) selecting at least one predefined standard, regulation and/or requirement with which the target system is to comply;

c) associating hardware and/or software information pertaining to the at least one device, collected in said step a), with at least one pre-defined platform category;

d) for each of said at least one platform category, determining which of one or more test procedures will be used to test hardware and/or software associated with said at least one platform category based on a mapping between the test procedures and the at least one predefined standard, regulation and/or requirement; and

e) generating one or more test procedures as determined in said step d) for each platform category.

50. The computer program medium according to claim 49 further comprising the step of associating at least one application software program with at least one platform category, the association indicating that the application program is typically installed on devices belonging to the platform category.

51. The computer program medium according to claim 49 wherein said step a) information is collected, for the target system comprising a plurality of devices within a network, by at least one of electronic discovery via a network and manual entry.

52. The computer program medium according to claim 51 wherein electronic discovery comprises an enterprise management system.

53. The computer program medium according to claim 51 wherein the information collected in said step a) pertains to at least one of: an internet protocol address, a hostname, a media access control address, an operating system name, and an operating system version.

54. The computer program medium according to claim 49 further comprising the step of editing said step a) information descriptive of at least the hardware specification and the operating system of each device.

55. The computer program medium according to claim 49 wherein the platform categories comprise at least one of desktop computer, laptop computer, mainframe computer, hub, handheld device, and other.

56. The computer program medium according to claim 49 further comprising the step of printing at least one test procedure generated in said step e).

57. The computer program medium according to claim 49 wherein said step e) generates one test procedure for a platform category when there are no devices associated therewith, and generates one test procedure for each device associated with a platform category having an indication that such device is to be tested.

58. The computer program medium according to claim 49 further comprising the steps of:

f) performing the steps associated with the test procedures generated in said step e) to determine whether the target system passes or fails the at least one the test procedure;

g) generating a score for each of a plurality of threat elements, each score indicating a likelihood of that threat element affecting and/or impacting the target system; and

h) (1) obtaining a threat correlation indication associated with said at least one test procedure, wherein said threat correlation indication indicates a relative potential of one or more given threats to exploit a vulnerability caused by a failure of the at least one test procedure, and

(2) determining a risk assessment by comparing each score generated in said step g) with a corresponding threat correlation indication of said step h) (1).

59. The computer program medium according to claim 58 wherein said scores for said step g) comprise at least one of:

i) negligible, wherein negligible indicates that the threat element is not applicable or has negligible likelihood of occurrence;

ii) low, wherein low indicates that the threat element has a relatively low likelihood of occurrence;

iii) medium, wherein medium indicates that the threat element has a medium likelihood of occurrence; and

iv) high, wherein high indicates that the threat element has a relatively high likelihood of occurrence.

60. The computer program medium according to claim 58 wherein said step g) threat elements comprise at least one of natural disaster elements, system failure elements, environmental failure elements, unintentional human elements, and intentional human elements.

61. The computer program medium according to claim 60 wherein the natural disaster threat elements comprise at least one of fire, flood, earthquake, volcano, tornado and lighting elements.

62. The computer program medium according to claim 60 wherein the system failure threat elements comprise at least one of a hardware failure, a power failure, and a communication link failure.

63. The computer program medium according to claim 60 wherein the environmental failure threat elements comprise at least one of temperature, power, humidity, sand, dust, shock, and vibration.

64. The computer program medium according to claim 60 wherein the human unintentional threat element comprises at least one of a software design error, a system design error, and an operator error.

65. The computer program medium according to claim 60 wherein the human intentional threat elements comprise at least one of an authorized system administrator, an authorized maintenance personnel, an authorized user, a terrorist, a hacker, a saboteur, a thief, and a vandal.

66. The computer program medium according to claim 60 wherein said step h) (1) threat correlation indication comprises at least one of the following scores:

i) negligible, wherein negligible indicates that the threat is not applicable to the vulnerability;

ii) low, wherein low indicates that the threat has a low potential to exploit the vulnerability;

iii) medium, wherein medium indicates that the threat has a potential to exploit the vulnerability; and

iv) high, wherein high indicates that the threat has a relatively high potential to exploit the vulnerability.

67. The computer program medium according to claim 66 wherein the risk assessment in said step h) (2) is determined in accordance with the following steps:

a) for each element in the project threat profile and corresponding element in the threat correlation pattern:

1) if a threat element score as determined in said step g) is negligible and a corresponding element in the threat correlation indication as determined in said step h) is anything, then the overall risk of the element is negligible;

2) if a threat element score as determined in said step g) is low and the corresponding element in the threat correlation indication as determined in said step h) is negligible, then the overall risk of the element is low;

3) if a threat element score as determined in said step g) is low and the corresponding element in the threat correlation indication as determined in said step h) is low, then the overall risk of the element is low;

4) if a threat element score as determined in said step g) is low and the corresponding element in the threat correlation indication as determined in said step h) is medium, then the overall risk of the element is low;

5) if a threat element score as determined in said step g) is low and the corresponding element in the threat correlation indication as determined in said step h) is high, then the overall risk of the element is medium;

6) if a threat element score as determined in said step g) is medium and the corresponding element in the threat correlation indication as determined in said step h) is negligible, then the overall risk of the element is negligible;

7) if a threat element score as determined in said step g) is medium and the corresponding element in the threat correlation indication as determined in said step h) is low, then the overall risk of the element is low;

8) if a threat element score as determined in said step g) is medium and the corresponding element in the threat correlation indication as determined in said step h) is medium, then the overall risk of the element is medium;

9) if a threat element score as determined in said step g) is medium and the corresponding element in the threat correlation indication as determined in said step h) is high, then the overall risk of the element is medium;

10) if a threat element score as determined in said step g) is high and the corresponding element in the threat correlation indication as determined in said step h) is negligible, then the overall risk of the element is negligible;

11) if a threat element score as determined in said step g) is high and the corresponding element in the threat correlation indication as

determined in said step h) is low, then the overall risk of the element is medium;

12) if a threat element score as determined in said step g) is high and the corresponding element in the threat correlation indication as determined in said step h) is medium, then the overall risk of the element is high; and

13) if a threat element score as determined in said step g) is high and the corresponding element in the threat correlation indication as determined in said step h) is high, then the overall risk of the element is high; and

b) selecting the risk profile for the failed test procedure as being the highest overall risk element.

68. The computer program medium according to claim 67, further comprising the step of determining an overall system risk.

69. The computer program medium according to claim 68 wherein the overall target system risk is the highest overall risk element of each of one or more failed test procedures.

70. The computer program medium according to claim 68 further comprising the step of printing a documentation package that will enable a determination to be made whether the target system complies with the at least one predefined standard, regulation and/or requirement selected in said step b).

71. The computer program medium according to claim 70 wherein the documentation package includes a risk assessment for at least one failed test procedure.

72. The computer program medium according to claim 70 wherein the documentation package includes an overall system risk.

73. A system for generating at least one test procedure for a target system having at least one device capable of being identified, each of the at least one device having hardware and/or software, said system comprising:

a) a discovery engine that scans the target system for the hardware configuration, operating system and/or application programs of each of the at least one device;

b) at least one storage medium for storing thereon at least:

(i) at least one predefined standard, regulation and/or requirement with which the segment is to comply; and

(ii) data pertaining to at least one platform category, each platform category having associated therewith one or more devices having at least a hardware specification and an operating system; and

c) decision logic for determining which of zero or more test procedures will be used to test each of the at least one platform category based on a mapping between the test procedures and the at least one predefined standard, regulation and/or requirement.

74. The system according to claim 73 further comprising a printer for printing the one or more test procedures.

75. The system according to claim 73 wherein the scanner collects for each device information pertaining to at least one of: an IP address, a hostname, a media access control address, operating system name, operating system version.

76. The system according to claim 73 wherein the scanner further collects information pertaining to at least one of application software, hard disk drive capacity, device manufacturer, and device model.

77. A system for generating at least one test procedure for a target system having at least one device capable of being identified, each of the at least one device having hardware and/or software, said system comprising:

a) a discovery engine that scans the target system information descriptive of at least a hardware and/or software specification for the at least one device;

b) a storage medium for storing at least one predefined standard, regulation and/or requirement with which the target system is to comply; and

c) a plurality of information entities, each of said plurality of information entities storing data pertaining to at least one predefined platform category, each platform category defining one or more devices having at least a hardware specification and an operating system; and

d) decision logic for determining which of one or more test procedures will be used to test each platform category based on a mapping between the test procedures and the at least one predefined standard, regulation and/or requirement.

78. The system according to claim 77 wherein said plurality of information entities comprise relational database tables.

79. The system according to claim 78 wherein said relational database tables comprise tables for defining: a) each of the at least one platform category; b) each of the at least one device; c) each application program; d) each defined association between an application program and a platform category, wherein each such association indicates that the application program is typically installed on devices belonging to the platform category; e) each defined association between an application program and a device, wherein each such association indicates that the application program is actually installed on the device; and g) each standard operating system.

80. A system for generating at least one test procedure for a target system comprising at least one device, each of the at least one device comprising a combination of hardware and software, said system comprising:

a) a discovery engine that scans the target system for at least a hardware and/or software specification for the at least one device;

b) at least one storage medium for storing thereon:

(i) at least one predefined standard, regulation and/or requirement with which the target system is to comply; and

(ii) data pertaining to at least one platform category, each platform category having associated therewith one or more devices having at least a hardware specification and an operating system; and

c) decision logic for:

i) associating hardware and/or software information pertaining to the at least one device, collected by said discovery engine, with at least one pre-defined platform category;

ii) for each of said at least one platform category, determining which of one or more test procedures will be used to test hardware and/or software associated with said at least one platform category based on a mapping between the test

procedures and the at least one predefined standard, regulation and/or requirement; and

iii) generating one or more test procedures as determined in said step ii) for each platform category.

81. The system according to claim 80 further comprising a printer for printing the one or more test procedures.

82. The system according to claim 80 wherein said network discovery engine collects for each device information pertaining to at least one of: an IP address, a hostname, a media access control address, operating system name, operating system version.

83. The system according to claim 83 wherein said network discovery engine further collects information pertaining to at least one of application software, hard disk drive capacity, device manufacturer, and device model.

84. A system for generating at least one test procedure for a target system having at least one device capable of being identified, each of the at least one device having hardware and/or software, said system comprising:

a) means for scanning the target system information descriptive of at least a hardware and/or software specification for the at least one device;

b) means for storing at least one predefined standard, regulation and/or requirement with which the target system is to comply; and

c) means for associating hardware and/or software information pertaining to the at least one device, collected by said means for scanning, with at least one pre-defined platform category;

d) for each of said at least one platform category, means for determining which of one or more test procedures will be used to test hardware and/or software associated with said at least one platform category

based on a mapping between the test procedures and the at least one predefined standard, regulation and/or requirement; and

e) means for generating one or more test procedures as determined in said step d) for each platform category.

85. A system for generating at least one test procedure for a target system comprising at least one device, each of the at least one device comprising a combination of hardware and software, said system comprising:

a) means for scanning the target system for at least a hardware and/or software specification for the at least one device;

b) means for storing thereon:

(i) at least one predefined standard, regulation and/or requirement with which the segment is to comply; and

(ii) data pertaining to at least one platform category, each platform category having associated therewith one or more devices having at least a hardware specification and an operating system; and

c) means for associating hardware and/or software information pertaining to the at least one device, collected by said discovery engine, with at least one pre-defined platform category;

d) for each of said at least one platform category, means for determining which of one or more test procedures will be used to test hardware and/or software associated with said at least one platform category based on a mapping between the test procedures and the at least one predefined standard, regulation and/or requirement; and

e) means for generating one or more test procedures, as determined by said means for determining, for each platform category.

86. A computer-assisted method of generating at least one test procedure for a target system having at least one device capable of being identified, each

of the at least one device having hardware and/or software, said method comprising the steps of:

a) collecting information descriptive of at least a hardware and/or software specification for the at least one device;

b) selecting at least one predefined standard, regulation and/or requirement with which the target system is to comply;

c) associating hardware and/or software information pertaining to the at least one device, collected in said step a), with at least one pre-defined platform category;

d) for each of said at least one platform category, determining which of one or more test procedures will be used to test hardware and/or software associated with said at least one platform category based on a mapping between the test procedures and the at least one predefined standard, regulation and/or requirement; and

e) generating one or more test procedures as determined in said step d) for each platform category;

f) performing the steps associated with the test procedures generated in said step e) to determine whether the target system passes or fails the at least one the test procedure;

g) generating a score for each of a plurality of threat elements, each score indicating a likelihood of that threat element affecting and/or impacting the target system; and

h) (1) obtaining a threat correlation indication associated with said at least one test procedure, wherein said threat correlation indication indicates a relative potential of one or more given threats to exploit a vulnerability caused by a failure of the at least one test procedure, and

(2) determining a risk assessment by comparing each score generated in said step g) with a corresponding threat correlation indication of said step h) (1).